Algebra 2: Exam presentations

Martin Sig Nørbjerg

June 7, 2022

1. Ideals, including maximal and prime ideals; ring homomorphisms.

Proposition 0.1. *Let R be a comm. ring and let $I \subset R$, be an ideal. Then I is a prime ideal if and only if R/I is a domain.*

Proof. " $\implies$ " Ass. I is a prime ideal. Let $[a], [b] \in R/I$ st. $[a][b] = 0$, this implies $ab \in I$. I is prime, thus $a \in I$ or $b \in I$ this implies that $[a] = 0$ or $[b] = 0$ in R/I (thus we have no zero divisors.)
" $\impliedby$ " Ass. I is not prime, then $\exists a, b \in R$ st. $ab \in I$ but $a, b \notin I$. Then $a + I \neq 0$ and $b + I \neq 0$ in R/I but $ab + I = 0$. Hence R/I is not a domain. ∎

Proposition 0.2. *Let R be a comm. ring and $I \subset R$ and ideal. then I is max iff R/I is a field.*

Proof. " $\implies$ " Ass. I is max and let $x \in R \setminus I$, then $x + I \neq 0$ in R/I since $x \notin I$. And I is thus strictly contained in $xR + I$, Since I is max, $xR + I = R \implies 1 \in xR + I$. Thus $\exists r \in R, i \in I$ st.

$$1 = xr + i \implies (x + I)(r + I) = 1 + I = [1]$$

This next part can be skipped
" $\impliedby$ " Ass. R/I is a field and let $I \subset J$. Let $x \in J \setminus I$, then $\exists y \in R$ st.

$$xy + I = (x + I)(y + I) = (1 + I).$$

then $1 - xy \in I \subset J$. But also $xy \in J$, hence $1 - xy + xy = 1 \in J$ which implies $J = R$. ∎

Remark 1. Every field is a domain, which implies that any maximal ideal is also prime.

2. Quotient rings, in particular $R[X]/\langle f\rangle$

Proposition 0.3. *Let $f : R \to S$ be a ring hom., then $ker(f)$ is an ideal.*

Theorem 0.4 (Gauss)**.** *Let $\mathbb{F}$ be a fin. field, and $G \subseteq \mathbb{F}^*$ a subgroup, then G is cyclic.*

Proposition 0.5. *Let $I \subset R$, be an ideal. I is maximal iff R/I is a field.*

Lemma 0.6. *Let $\mathbb{F}$ be a fin. field. Then $|\mathbb{F}| = p^n$ where $n \geq 1$ and p prime. There $\exists$ irr. $f \in \mathbb{F}_p[x]$ with $deg(f) = n$ st. $\mathbb{F} \cong \mathbb{F}_p[x]/\langle f\rangle$.*

Proof. $Char(\mathbb{F}) = p$ prime $\implies$ $\mathbb{F}_p$ is a subring of $\mathbb{F}$. $\mathbb{F}^*$ is a cyclic group, by the theorem. Let $\gamma \in \mathbb{F}^*$ be the generator. (Thus every element in $\mathbb{F}$ is either 0 or some power n of γ.) Consider the hom. $\varphi : \mathbb{F}_p[x] \to \mathbb{F}$, defined as $\varphi(x) = \gamma$, then

$$\varphi\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} a_k \gamma^k$$

which $\implies$ φ is surj (since $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$, however $\varphi(0) = 0$). Now $ker(\varphi)$ is an ideal of $\mathbb{F}_p[x]$, but $\mathbb{F}_p[x]$ is a Euclidean domain and thus a PID. which $\implies$ $\exists f \in \mathbb{F}_p[x]$ st. $ker(\varphi) = \langle f\rangle$. Thus by the ring isomorphism theorem

$$\mathbb{F}_p[x]/\langle f\rangle \cong \mathbb{F}$$

which $\implies$ $\langle f\rangle$ is maximial, by the proposition. This $\implies$ f is irr. (since $\langle x\rangle \subseteq R$ is max. ideal iff x irr. in R) Now $|\mathbb{F}| = p^n$ implies $deg(f) = n$ ∎

3. Types of rings: UFD, PID, Euclidian domains

Proposition 0.7. *Let R be a ring st. all $r \in R \backslash R^*$, $r \neq 0$. has a fac. into irr. elem. Then every irr. elem in R is prime iff R is UFD.*

Lemma 0.8. *Let R be a PID and $r \in R \backslash R^*$ and $r \neq 0$. Then r has a fac. into irr. elem.*

Proposition 0.9. *Let R be PID, that is not a field. Then $x \in R$ is irr. iff $\langle x \rangle$ is max.*

Skip the proof

Proof. " $\Longrightarrow$ " Let x be irr. and $\langle x \rangle \subseteq \langle y \rangle$. then

$$\exists z \in R \text{ st. } zy = x \implies y|x \implies \exists s \text{ st. } sy = x$$

now x being irr. implies either $s \in R^* \implies \langle x \rangle = \langle y \rangle$ or $y \in R^* \implies \langle y \rangle = R$, since y unit implies $1 \in \langle y \rangle$. Thus $\langle x \rangle$ is max.
" $\Longleftarrow$ " Let $\langle x \rangle$ be max. Then $x = y \cdot s$ implies

$$\langle x \rangle \subseteq \langle y \rangle \implies \begin{cases} \langle y \rangle = \langle x \rangle \implies s \in R^* \text{ (x and y are associative)} \\ \langle y \rangle = R \implies y \in R^* \end{cases}$$

which implies x is irr. ∎

Theorem 0.10. *Let R be a PID, then R is a UFD.*

Remark 2. Note here that a field is trivially a UFD, since all elems. are units. Thus we can assume R is not field.

Proof.

i) By the pervius lemma, all $r \in R \backslash R^*$, $r \neq 0$, has a fac.

ii) We show that this fac. is uniq. by showing that all irr. are prime and thus by the first prop. R is a UFD.

iii) Let $x \in R$ be irr. and assume $x|ab$ and $x \nmid a$, then $a \notin \langle x \rangle$ and hence $\langle x \rangle \subset \langle x, a \rangle$, by the previus lemma $\langle x \rangle$ is max. and hence $\langle x, a \rangle = R$. Hence $\exists r, s \in R$ st. $rx + sa = 1$ multiplying by b we get

$$b(rx + sa) = brx + sab = b$$

since $x|ab$ it follows that $x|b$, thus x is prime.

∎

4. Gaussian integers and Fermats two-square theorem.

Proposition 0.11. *Let R be a ring st. all $r \in R \backslash R^*$, $r \neq 0$. has a fac. into irr. elem. Then every irr. elem in R is prime iff R is UFD.*

Proposition 0.12. *Let $\pi \in \mathbb{Z}[i]$, with $N(\pi) = p$, p prime. Then π is a prime in $\mathbb{Z}[i]$.*

Proof. The gaussian integers is a Euclidian domain, $\therefore$ it's a unq. fac. domain. Thus every irr element is a prime element. Thus it's sufficient to show that π is irr. Ass. $\pi = ab$, then

$$N(\pi) = N(ab) = N(a)N(b) = p$$

since N is a hom. Ass. WLOG that $N(a) = p$, then $N(b) = 1$ and b is thus a unit since $Z[i]^* = \{1, -1, i, -i\}$. ∎

Theorem 0.13 (Fermat two-square)**.** *For prime numbers $p \equiv 1 \ (mod\ 4)$ there $\exists! a, b \in \mathbb{Z}$ st. $a^2 + b^2 = p$.*

Proof. We prove the unq.:
Ass. $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ and $p = c^2 + d^2$ for some other $c, d \in \mathbb{Z}$. Then

$$p = (a + ib)(a - ib) = (c + id)(c - id)$$

however by the proof of prop,

$$(a + ib), (a - ib), (c + id), (c - id)$$

are all irr. Since

$$N(a + ib) = N(a - ib) = N(c + id) = N(c - id) = p$$

gives two irr. fac. of p, however $\mathbb{Z}[i]$ being a Euclidian domain implies it is a UFD, and thus the fac. is the same upto multiplication by units. ∎

5. Cyclotomic polynomials and roots of unity

Lemma 0.14. *$\xi \in \mathbb{C}$ is a primitive n'th root of unity iff*

$$\xi = \mathrm{e}^{2k\pi i/n},$$

st. $1 \leq k \leq n$ and $gcd(k, n) = 1$. If ξ is a primitive n'th root of unity and $\xi^m = 1$ then $n|m$.

Theorem 0.15. *Let R be a domain and $f \in R[X]\backslash\{0\}$. If $V(f) = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ then.*

$$f = q \prod_{k=1}^{r} (X - \alpha_k)^{v_{\alpha_k}(f)}$$

where $q \in R[X]$ and $V(q) = \emptyset$. And $\sum_{k=1}^{r} v_{\alpha_k}(f) \leq deg(f)$.

Proposition 0.16. *Let $n \in \mathbb{N}$. Let $f = X^n - 1$ and $g = \prod_{d|n} \Phi_d(X)$ then $f = g$*

Proof.

i) Both f and g are monic $\therefore$, they are equal if they both have the same roots, with the same multiplicites, this follows from theorem. Since f monic $\implies$ $q = 1$ in the thm.

ii) We will now proof that f and g have the same roots with the same multiplicites. The roots of g is the d'th primitive roots of unity st. $d|n$, these are also roots of f: Let x be a root of g then

$$d|n \implies \exists k \in \mathbb{Z} \text{ st. } d \cdot k = n \implies x^n = x^{d \cdot k} = 1^k = 1.$$

Now ξ begin a root of f means ξ is a n'th root of unity, however this implies that ξ is a d'th primitive root of unity, where $d|n$, consult the lemma. Thus ξ is also a root of g. Lastly none of the roots have multiplicty higher than one.

■

6. Quadratic reciprocity

Definition 0.17. Let p prime and $a \in \mathbb{Z}$ st. $p \nmid a$. Then a is a quadratic residue modulo p if there $\exists x \in \mathbb{Z}$ st. $x^2 = a \pmod{p}$. Also the legendre symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a QR} \\ -1 & \text{otherwise.} \end{cases}$$

Proposition 0.18. *Let p prime, st. $p \neq 2$, then half the numbers $1, 2, \ldots, p-1$ are QR.*

Proof. Let $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^*$ be defined by $\varphi : n \mapsto n^2$. Then φ is a group hom. (with $\cdot$ as operation). Now $ker(\varphi) = \{-1, 1\}$. Now by the ring isomorphism theorem

$$Im(\varphi) \cong \mathbb{F}_p^* / ker(\varphi)$$

However this implies that $|Im(\varphi)| = \dfrac{p-1}{2}$. ∎

Lemma 0.19. *Let p be prime, and $x \in \mathbb{Z}$, then*

$$x^2 \equiv 1 \pmod{p} \implies x \equiv \pm 1 \pmod{p}$$

Theorem 0.20. *Let p prime, st. $p \neq 2$ and $p \nmid a$ then $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$*

Proof. If a is a quadratic residue then $\exists x \in \mathbb{Z}$ st. $x^2 \equiv a \pmod{p}$. Thus

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod{p}$$

by Eulers theorem ($a^{\varphi(n)} \equiv 1 \pmod{n}$), where $\varphi(p) = p-1$, this is also known as (Fermats little theorem). However $\left(\dfrac{a}{p}\right) = 1$ which concludes this case. $x^{\frac{p-1}{2}} - 1$ has at most $\frac{p-1}{2}$ roots, so non quadratic residues cannot be roots, since there are $\frac{p-1}{2}$ quadratic residues by the prop. However $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \pmod{p}$ for all $a \in \mathbb{Z}$. By the lemma this implies

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

however the quadratic residues are the solutions to the equation $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, thus $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, when x is not a quadratic residue. ∎

7. Finite fields, including the existence and/or uniqueness

Theorem 0.21. *For all $n \geq 1$ and p, prime, there $\exists$ irr. $f \in \mathbb{F}_p[x]$, with $deg(f) = n$*

Corollary 0.22. *For all $n \geq 1$ and p, prime, there exists a fin. field $\mathbb{F}$ with $|\mathbb{F}| = p^n$.*

Proof. there $\exists$ irr poly $f \in \mathbb{F}_p[x]$ with $deg(f) = n$, now let $\mathbb{F} = \mathbb{F}_p[x]/\langle f \rangle$, then $|\mathbb{F}| = p^n$ and $\mathbb{F}$ is field, since f irr. ∎

Lemma 0.23. *Let $\mathbb{F}$ be a fin. field. there $\exists$ irr. $f \in \mathbb{F}_p[x]$ with $deg(f) = n$ st. $\mathbb{F} \cong \mathbb{F}_p[x]/\langle f \rangle$.*

Theorem 0.24. *If $|\mathbb{F}| = |\mathbb{F}'| = p^n$ then $\mathbb{F} \cong \mathbb{F}'$.*

Proof. We have that $\mathbb{F} \cong \mathbb{F}_p[x]/\langle f \rangle$ for f irr. with $deg(f) = p^n$. Let $\alpha = [x]$, so $f(\alpha) = 0$. Consider $I = \{g \in \mathbb{F}_p[x] \mid g(\alpha) = 0\} \subset F_p[x]$, then I is an ideal and $f \in I$. Which $\implies \langle f \rangle \subseteq I$ but f irr. $\implies \langle f \rangle$ max. and thus $\langle f \rangle = I$.
Since $\xi^{p^n} = \xi(\xi^{p^n - 1}) = \xi \cdot 1 = \xi$ we have $x^{p^n} - x \in I$ and thus $f \mid x^{p^n} - x$.

In $\mathbb{F}'[x]$ we can find $x^{p^n} - x = \prod_{\beta \in \mathbb{F}'} (x - \beta)$ since $\beta^{p^n} = \beta$ for all $\beta \in \mathbb{F}'$ $\therefore$ $f \in \mathbb{F}_p[x] \subseteq \mathbb{F}'[x]$ has a root $\alpha' \in \mathbb{F}'$, since it devides $x^{p^n} - x$. Consider the hom. $\varphi : \mathbb{F}_p[x] \to \mathbb{F}'$, defined as $x \mapsto \alpha'$, then $\langle f \rangle \subseteq ker(\varphi)$, since $\varphi(f) = f(\alpha') = 0$. But $ker(\varphi) \neq \mathbb{F}_p[x]$ and by the maximality of $\langle f \rangle$ we have that $\langle f \rangle = ker(\varphi)$. $\therefore$ we get an inj. ring hom.

$$\tilde{\varphi} : \mathbb{F}_p[x]/\langle f \rangle \to \mathbb{F}'$$

but since $|F_p[x]/\langle f \rangle| = |\mathbb{F}'|$, $\tilde{\varphi}$ must be surj. And thus we have

$$\mathbb{F} \cong \mathbb{F}_p[x]/\langle f \rangle \cong \mathbb{F}'$$

∎

8. Berlekamps algorithm

Proposition 0.25. *Let $f \in \mathbb{F}_p[x]$ be non constant, and let $deg(f) = d$. Then $\mathbb{F}_p[x] \setminus \langle f \rangle$ is a $\mathbb{F}_p$ vec space of dim d.*

Theorem 0.26. *Let $f \in \mathbb{F}_p[x]$ be a non-constant poly, let $R = \mathbb{F}_p[x]/\langle f \rangle$ and $F : R \to R$ be the frobenius map. Then f is irr. iff $ker(F) = \{0\}$ and $ker(F - I) = \mathbb{F}_p$*

Proof. " $\Longleftarrow$ " Assume $ker(f) = \{0\}$ and $ker(F - I) = \mathbb{F}_p$. We will proof that f is irr. by showing that R is a field. Let $a \in R$ st. $a \neq 0$, define $\varphi : R \to R$ as $x \mapsto a \cdot x$. Now let $x \in ker(\varphi) \cap Im(\varphi) \neq \emptyset$, since 0 is in the set. Then $x = ay$ for some $y \in R$ and $ax = 0$.

$$F(x) = F(ay) = a^p y^p = (a^{p-1} y^{p-1})(ay) = (a^{p-2} y^{p-1}) ax = 0$$

However $ker(F) = \{0\}$ by our ass. and thus $x = 0 \implies ker(\varphi) \cap Im(\varphi) = \{0\}$ and since $ker(\varphi) + Im(\varphi) = R$, by the fondemental theorem of linear maps. We have

$$ker(\varphi) \oplus Im(\varphi) = R$$

thus we can write $1 = \alpha + \beta$ where $\alpha \in ker(\varphi)$ and $\beta \in Im(\varphi)$. We have

$$\varphi(F(\alpha)) = a\alpha^p = \varphi(\alpha)\alpha^{p-1} = 0, \text{ since } \alpha \in \ker(\varphi)$$

which $\implies F(\alpha) \in ker(\varphi)$. Now $\beta \in Im(\varphi) \implies \exists y \in R$ st. $\beta = ay$ and

$$F(\beta) = \beta^p = a(a^{p-1} y^p) \in Im(\varphi)$$

Now since $F(\alpha) + F(\beta) = F(\alpha + \beta) = F(1) = 1$ thus since the sum is direct, we have $F(\alpha) = \alpha$ and $F(\beta) = \beta$. However this implies $F(\alpha) - \alpha = F(\beta) - \beta = 0$ which $\implies \alpha, \beta \in ker(F - I) = \mathbb{F}_p$ by our ass. Now $\alpha \in ker(\varphi) \implies \alpha = 0$ since $a \neq 0$ and we are dealing with a field, which is a domain. However $\beta = 1$ and $\beta \in Im(\varphi) \implies 1 \in Im(\varphi)$ and thus there $\exists y \in R$ st. $1 = a \cdot y$. Thus a is invertible which $\implies R$ is a field which $\implies f$ is irr. ■